

## **AFFIDAVIT OF MATTHEW K. O'NEILL**

I, Matthew K. O'Neill, being first duly sworn, hereby depose and state as follows:

### **I. INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since 1998. I received formal training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, and the United States Secret Service Academy in Beltsville, Maryland. I am currently assigned to the United States Secret Service, Manchester Resident Office. My current assignment includes investigating violations of Title 18, United States Code, Sections 1028, 1029, 1030, 1341, 1343, 1344 and 1956 on the internet. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

2. As set forth herein, the USSS is currently investigating individuals who are hacking into the computer terminals of retailers, and in turn stealing their login credentials to a credit report database owned by Experian, one of the largest such credit profile databases in the world. The bad actors then query individuals to obtain their full credit report, which includes personal information such as name, date of birth, social security number, address, and bank account information, all in violation of 18 U.S.C. §§ 1028 (identity fraud), 1029 (access device fraud), 1030 (computer fraud and abuse), and 1343 (wire fraud). A number of the individuals who had their credit reports queried are residents of New Hampshire.

3. The investigation to date has identified more than 55 compromised Experian credentials that were assigned to businesses and over 12,000 credit reports have been queried. Some of these other compromised merchants include Stamford Postal Credit Union, Chief Financial Credit Union, Palm Desert National Bank, Saratoga Homes, Morongo Band of Mission Indians Casino Resort and Spa, Verizon Wireless, Sallie Mae, El Paso Police Academy, and the Paterson Police Federal Credit Union.

4. As set forth below, using **rr2518@gmail.com**, a target has discussed and provided access to stolen personal identifying information (PII).

5. I am submitting this affidavit in support of an Application for a Search Warrant to search records and other information (including the contents of communications) associated with a certain account, specifically: **rr2518@gmail.com**, that is stored at premises owned, maintained, controlled, or operated by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (hereafter "Google"). The information to be searched is described in the following paragraphs and in Attachment A.

6. Based on my training and experience, and the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of Title 18, United States Code, Sections 1028, 1029, 1030 & 1343 have been committed by unknown targets/suspects. There is also probable cause to believe that records and other information associated with e-mail account **rr2518@gmail.com** as described in Attachment A, contain evidence, fruits, and

instrumentalities of various violations of Title 18, United States Code, Sections 1030, 1028 & 1343, as detailed and specified herein below. Accordingly, there is probable cause to search the information described in Attachment A for evidence, fruits, and/or instrumentalities of these crimes, as described in Attachment B. This affidavit is made in support of an Application for a Search Warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to compel Google, a provider of electronic communication and remote computing services, to provide certain items as set forth in Attachment B, Part I, hereto, and for the government to search and to seize certain items as set forth in Attachment B, Part II, hereto.

7. The facts set forth in this affidavit are based upon my personal observations, my review of documents and computer records, my training and experience, and information obtained from other agents and witnesses, including from Romanian law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge of the investigation into this matter.

## **II. PROBABLE CAUSE**

8. Your affiant believes that there is probable cause to believe that evidence, instrumentalities, and fruits of criminal activity will be found in a search of computer servers hosted at Google, for the following reasons. In or about November 2010, the USSS was notified by Experian that they were experiencing losses due to unauthorized credit report queries on customers' accounts. The accounts that had apparently been compromised had been assigned to various merchants such as credit unions, banks, and other merchants that perform credit checks. Over 50 merchants had their Experian login credentials stolen and over 12,000 credit reports have been queried by the bad actors.

9. Further investigation, including interviews with representatives of financial institutions, third party forensic examiners, and individual victims, revealed that the Experian login credentials were stolen after the merchant was compromised via malware such as Zeus. In fact, Zeus malware variants were identified in the majority of the compromises in which the suspect malware was located.

10. Further investigation, including interviews with representatives from Experian's corporate headquarters, has identified at least eight New Hampshire residents who had their credit reports queried without authorization using one of the aforementioned compromised login credentials.

11. Throughout this investigation, I have communicated regularly with Investigator Scott Moore, Experian, a company located in California that is one of the three main credit bureaus in the United States. I have communicated with other Experian information technology (IT), and investigative, representatives as well. Experian clients have engaged third-party computer forensic examination firms, which have conducted various forensic examinations on the compromised terminals. I have reviewed reports summarizing the findings of those examinations.

12. As a result of my discussions with Moore and review of written materials provided by Moore and others at Experian relating to his investigative activities, I have learned that various types of malicious software called "keystroke loggers" ("KSL") had been installed on Experian's clients computers, that the programs were storing login credentials, and that the programs were uploading the data from the victim merchant's terminals to another location to be used to query credit reports.

13. During the course of the investigation it has been learned that a website identified as findget.me offers to sell personal information in a searchable format. The website states that anyone can purchase someone's identifiers; such as first name/last name/middle name/e-mail address/e-mail password/address/phone/DOB/Drivers License #/Bank Name/Bank account number/Bank Routing Number/Company name/Current years on job/mother's maiden name. Open source searches advise that this site is hosted by Westhost, 164 North Gateway Drive, Providence, UT 84332. The contact e-mail address for this site is **rr2518@gmail.com**.

14. Using an undercover gmail account, I sent an e-mail to **rr2518@gmail.com** asking for login credentials to findget.me. I received a response from **rr2518@gmail.com**, which included a username and password, which allowed me to enter this site. This e-mail account, **rr2518@gmail.com**, is the only e-mail address or contact information listed on this site and is listed as the site's administrator.

15. On November 29, 2011, I purchased 245 unique identifiers for individuals residing in the United States on findget.me. The identifiers include first name/last name/middle name/e-mail address/e-mail password/address/phone/DOB/Drivers License #/Bank Name/Bank account number/Bank Routing Number/Company name/Current years on job/mother's maiden name. I paid \$40 for all 245 individuals PII. Findget.me advises that this information came from an "old" database. I also purchased 50 unique identifiers for individuals residing in the United States. The identifiers include first name/last name/middle name/e-mail address/e-mail password/address/phone/DOB/Drivers License #/Bank Name/Bank account number/Bank Routing Number/Company name/Current years on job. Findget.me advises that this information came from a "fresh" database but does not include mother's maiden name. I paid \$12.50 for all 50 individuals PII. I paid findget.me through an account at libertyreserve.com, which is the only acceptable payment source for findget.me. The 245 and 50 sets of personal identifying information was not searchable and was provided to me through the website as a txt file. I also purchased PII, which included name, date of birth, address, and social security number for over 15 individuals who were previously queried, without permission, using the stolen Experian login credentials through findget.me's searchable database. The information that is returned also lists a "SourceID", "date reported", "date created", and "date updated." In some instances, the "SourceID" is "EX." Other "SourceIDs" include MV, TH, NCO, and TU.

16. On or about December 5, 2011, I sent \$25 to a Liberty Reserve account that **rr2518@gmail.com** specified as belonging to him. The purpose of the payment was to purchase unique identifiers for individuals specifically residing in New Hampshire. On the same date, I received an email from **rr2518@gmail.com** that contained a .txt attachment. The body of the email said "thx you." The attachment contained approximately 90 unique identifiers for New Hampshire residents. Below is an example of the information I received for each New

Hampshire resident. The personal information that I received includes name, date of birth, email address, email address password, address, telephone number, date of birth, social security number, bank name, bank account number, bank routing number, employer, and years employed at employer. By way of limited example, a redacted copy of one such individual's information I received is set forth below, with some information redacted by the insertion of Xs in place of letters or numbers that appear in the original:

Line 26654: | 3XXXX0 | Dec 10 2010 12:00AM | Rejected | NA | genna | fielders | |  
 gfXXXorXXXX@aol.com | geXXX1 | 13 XXXXXXXX AVE | | RAYMOND | New  
 Hampshire | 03077 | (603)396-XXXX | 08/XX/19XX | 020-XX-XXXX | 0XfsXXX111 |  
 citizens bank | 18XX | XXX629XXXX | 0XX40XXX3 | prudential | 10 Year(s) 8  
 Month(s) | |

17. In my experience, the sale of such personal identifying information cannot be done legally.

18. Based on: (A) my review of the records and other evidence obtained to date in this investigation; (B) the fact that the person who gave me access to the site findget.me by sending me an e-mail that contained my userid and password information to enter findget.me, and who sold me PII has used the e-mail address **rr2518@gmail.com**; and, (C) the fact that the e-mail account **rr2518@gmail.com** is listed as the main contact and administrator for the site findget.me, I believe that there is probable cause to believe that the suspect e-mail account, **rr2518@gmail.com** contains fruits, instrumentalities and evidence of the identity theft scheme.

### III. TECHNICAL BACKGROUND

19. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the e-mail account, **rr2518@gmail.com**, listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information.

20. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on a Google server indefinitely.

21. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on a Google server indefinitely.

22. A sent or received e-mail typically includes the content of the message, source

and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

23. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google.

24. Subscribers to Google might not store on their home computers copies of the e-mails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

25. In general, e-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

26. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

27. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

28. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

#### **IV. RELEVANT FEDERAL OFFENSES**

29. Based upon the information above, your affiant believes that there is probable cause to believe that on the computer systems owned, maintained, and operated by Google, as described above, there exists evidence, fruits, and/or instrumentalities of violations of Title 18



United States Code, Section 1028 - Fraud In Connection with Access Devices; 1029 – Identity Theft; Section 1030 - Fraud In Connection with Computers; and Section 1343 -Wire Fraud, allowing agents to seize records and other information (including content of communications) stored on servers being maintained by Google for the account and files associated with the e-mail account: **rr2518@gmail.com**.

## **V. LEGAL AUTHORITY AND INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

30. If issued, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) located at the premises described in Attachment A (“Place to Be Searched”) and particularly described in Attachment B, Part I (“Information to Be Disclosed by Google”). Upon receipt of the information described in Part I of Attachment B, government-authorized persons will review that information to locate the items described in Part II of Attachment B (“Information to Be Seized by the Government”).

31. The government may obtain internet and e-mail content and subscriber information from a third party by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). Any court with jurisdiction over the offense under investigation may issue a § 2703 warrant, regardless of the location of the server where information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike Rule 41 search warrants, a § 2703 warrant does not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

32. If the government obtains a search warrant, there is no requirement that the third party give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), (c)(3).

## **VI. CONCLUSION**

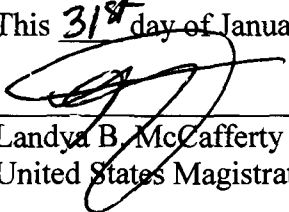
33. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that unknown targets have committed access device fraud, in violation of 18 U.S.C. § 1028, identity theft, in violation of 18 U.S.C. § 1029, computer fraud and abuse, in violation of 18 U.S.C. § 1030, and wire fraud, in violation of 18 U.S.C. § 1343. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that computer systems owned or operated by or in the control of Google, an e-mail service provider located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, contain evidence, fruits, and instrumentalities of the crimes identified above. Accordingly, a Search Warrant is requested.

34. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

*Matthew K. O'Neill*

Special Agent Matthew K. O'Neill  
United States Secret Service

Subscribed and sworn to before me  
This 31<sup>st</sup> day of January, 2012

  
\_\_\_\_\_  
Landya B. McCafferty  
United States Magistrate Judge